Improving Bit Generation Rates for Quantum Random Number Generators

Walter O. Krawec[a]

[a]University of Connecticut, Storrs, CT, USA

ABSTRACT

Quantum Random Number Generators (QRNG) are quantum cryptographic protocols that distill secure random bit strings from quantum sources. One of the main research challenges in this area is to improve their random bit generation rates. Here we investigate several possible post processing strategies for QRNG protocols, showing when they help and when they hinder. We also look at the trade-offs to using these methods as some require a larger amount of initial randomness. Finally, we comment on some interesting future problems that remain open.

1. INTRODUCTION

Quantum cryptography allows for security against computationally unbounded adversaries, something often not possible in the classical world. While Quantum Key Distribution (QKD) is perhaps the most celebrated of these results, a close relative, Quantum Random Number Generation (QRNG), are also a vital cryptographic primitive. Here, quantum states and measurements are used to produce a random string that is (1) uniform random and (2) independent of any adversary system. See[1] for a survey of QRNG protocols. See also[2,3] for a general survey on quantum cryptography.

Many security models exist for QRNG protocols from the fully trusted device model (leading to systems with weak security guarantees, but fast bit generation rates) to the opposite extreme of complete device independence (leading to systems with strong security, but slow bit generation rates using today's technologies).[4,5] A middle ground is the source-independent (SI) model, originally introduced in[6] and studied in various follow up works including.[7–12] This allows a strong security guarantee, while also fast and highly efficient implementations and bit generation rates.

In this work, we study classical post processing methodologies to improve bit generation rates of these source independent QRNG protocols. Post processing has been shown to drastically improve performance of QKD protocols. However, in this work, we show the story is not as clear cut in the QRNG case. In particular, we show how some QKD post processing strategies can actually hurt QRNG performance. We also introduce some novel quantum post processing strategies which can greatly improve the performance of the system under investigation.

2. PRELIMINARIES

We first introduce some basic notation and terminology used throughout this work. We use $|\phi_i\rangle$ to represent the four Bell states, namely:

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$
$$|\phi_1\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$
$$|\phi_2\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$
$$|\phi_3\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

Further author information: (Send correspondence to W.O.K.)
W.O.K.: E-mail: walter.krawec@uconn.edu

Quantum Information Science, Sensing, and Computation XV, edited by Eric Donkor, Michael Hayduk, Carlos M. Torres, Proc. of SPIE Vol. 12517, 1251707
 · 0277-786X · doi: 10.1117/12.2663504

Let ρ_{AE} be a quantum state or density operator, namely a positive semi-definite Hermitian operator of unit trace acting on some Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_E$. We write ρ_E to mean the operator resulting from tracing out the A register, namely $\rho_E = tr_A \rho_{AE}$. We write $H(AE)_\rho$ to mean the von Neumann entropy of the density operator ρ_{AE}, namely:

$$H(AE)_\rho = -tr\rho_{AE} \log_2 \rho_{AE}.$$

Let X be a classical random variable which has outcome x_i with probability p_i. Then the Shannon entropy of this variable is denoted $H(X)$ (without the quantum state subscript used to distinguish with von Neumann entropy) and is defined to be $H(X) = -\sum_i p_i \log_2 p_i$. If $\{\lambda_i\}$ are the eigenvalues of ρ_{AE}, then $H(AE)_\rho = H(\lambda_1, \cdots, \lambda_n) = -\sum_i \lambda_i \log_2 \lambda_i$.

In quantum cryptography, one often has a classical-quantum state ρ_{AE} - i.e., a state where the A register contains classical data while the E register is quantum. One may run a privacy amplification process on the A register which involves choosing a random two-universal hash function and applying that function to the A register, creating a new classical-quantum state σ_{KE} (see[13]). Here the bit-length of the K register is ℓ, which is no greater than, and often much shorter than, the bit-length of the original A register (which we denote for now by $n \geq \ell$). As shown in,[13] it holds that, following privacy amplification:

$$\left|\left|\sigma_{KE} - I/2^\ell \otimes \sigma_E\right|\right| \leq \sqrt{2^{-(H_\infty(A|E)_\rho - \ell)}},$$

where $H_\infty(A|E)_\rho$ is the *quantum min entropy* defined in.[13] The above result says, roughly, that the size of the final secret string ℓ is approximately equal to the min entropy of the state before privacy amplification. As we are only interested in the asymptotic case, where $n \to \infty$, we actually have that a secret key may be extracted of relative size:[13]

$$\lim_{n\to\infty} \frac{\ell}{n} = H(A|E)_\rho. \tag{1}$$

The above expression is called the bit generation rate of a QRNG protocol and is denoted `rate`. Another important metric is the *effective* bit generation rate defined to be the ration of secret random bits over the total number of signals sent $N \geq n$. In the asymptotic case $N \approx n$ often (and so the effective rate is the same as the bit rate), but this is not always the case as we see later.

3. PROTOCOLS

We investigate two SI-QRNG protocols. The first is a protocol introduced in.[6] We denote this protocol by $\texttt{QRNG}_1$ and it operates as follows:

1. A source, Eve (which is potentially adversarial), prepares an N- qubit signal $|\psi\rangle_{AE}$, where the A portion consists of an N-qubit signal and the E portion is a private ancilla held by the adversary. If the source is honest, the state prepared should be $|\psi\rangle_{AE} = |+\rangle^{\otimes N} \otimes |0\rangle_E$, that is, the A portion should be N copies of $|+\rangle$ while the E portion remains independent of the signal sent to the user Alice.

2. The receiver, Alice, receives the N qubit register A and selects some portion of the signals to Test and the rest to Distill. For those qubits she chooses to Test, she measures in the X basis resulting in outcome $q \in \{0,1\}^m$ (where an observation of $|+\rangle$ is translated to an outcome of 0). For those she chooses to Distill, she measures in the Z basis receiving outcome $r \in \{0,1\}^{N-m}$. Note that, if the source is honest, it should hold that $q = 0 \cdots 0$ and r should be a uniform random string. Let Q_X be the overall noise in the signal.

3. The receiver, Alice, performs a post-processing protocol (to be discussed and is optional). This takes as input q and r and outputs a new bit string $r' \in \{0,1\}^n$ with $n \leq N - m$. Note that if post-processing is not used, it simply holds that $r' = r$.

4. The receiver, Alice, then takes r' and performs a privacy amplification process, hashing this string r' down to a secret random string s of size $\ell \leq n$.

The second protocol was introduced in[7] and we denote it by $\texttt{QRNG}_2$. It operates as follows:

1. A source, Eve (which, again, may be adversarial) prepares a quantum state $|\psi\rangle_{AE}$ where the A register consists of $2N$ qubits. If the source is honest, the state prepared should be of the form $|\psi\rangle_{AE} = |\phi_0\rangle^{\otimes N} \otimes |0\rangle_E$. That is, if the source is honest, the state should be N copies of the Bell state $|\phi_0\rangle$ and Eve's ancilla should be independent.

2. The receiver, Alice, chooses some of the qubit pairs as a Test; for these rounds, Alice measures each qubit in the pair in either the Z basis, the X basis, or optionally the Y basis. If the source is honest, these measurement outcomes for each individual pair should be fully correlated. We denote by Q_Z, Q_X, and Q_Y to be the percentage of outcomes in each individual basis test that are not correlated (if the source is honest, each of these values should be zero - that is, these values represent the "noise" in the signal). The remaining qubit pairs are used to Distill a random string. For this, Alice measures the first qubit of each pair in the Z basis leading to a random string r. The second qubit from each pair is discarded.

3. The receiver runs an optional post-processing stage, taking as input Q_Z, Q_Y, Q_X, and r and outputs r'.

4. The final random string r' is run through privacy amplification to output a final random string s.

We note that step 3 of each of the above protocols is new - the original specifications of these protocols did not include a post-processing stage. The purpose of this work is to investigate the performance of different post processing protocols when used for each of these protocols to see when or if there is a benefit.

4. CLASSICAL POST-PROCESSING

We first consider classical post-processing methods for $\texttt{QRNG}_1$. The first method is inspired by a QKD post processing method discussed in[14] which increased the noise tolerance of QKD protocols. It turns out for QRNG these methods are not as helpful unless the noise can be added naturally. The second method involves two quantum sources which can provide some benefits for QKD and is based on the multi-mediated server method introduced in[15] for QKD. Again, the QRNG scenario is different.

4.1 Adding Noise to the String

The first post processing strategy we consider is based on one discussed in[14] for QKD. The process is as follows:

- Given a raw string $r \in \{0,1\}^n$, for every bit r_i, set $r'_i = r_i$ with probability $1-p$, otherwise, with probability p, set $r'_i = 1 - r_i$.

We analyze the asymptotic case here and, so compute the von Neumann entropy under collective attacks (de Finetti style arguments, then, may be used to promote the analysis to general attacks[16]). Consider a source that prepares N copies of the state $|\psi_0\rangle$:

$$|\psi_0\rangle = \sum_{a=0}^{1} \alpha_a |a, e_a\rangle , \tag{2}$$

where each $|e_a\rangle$ is a normalized state. We may assume that the state is symmetric in the sense $\alpha_0 = \alpha_1 = 1/\sqrt{2}$ (this may be enforced by users) and so the state takes on the form:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}} |0, e_0\rangle + \frac{1}{\sqrt{2}} |1, e_1\rangle .$$

Given this, the probability that Alice observes $|-\rangle$ on a Test round is easily seen to be:

$$Q_X = \frac{1}{2}(1 - Re\,\langle e_0|e_1\rangle)$$

We may write

$$|e_1\rangle = \alpha |e_0\rangle + \beta |f_0\rangle , \tag{3}$$

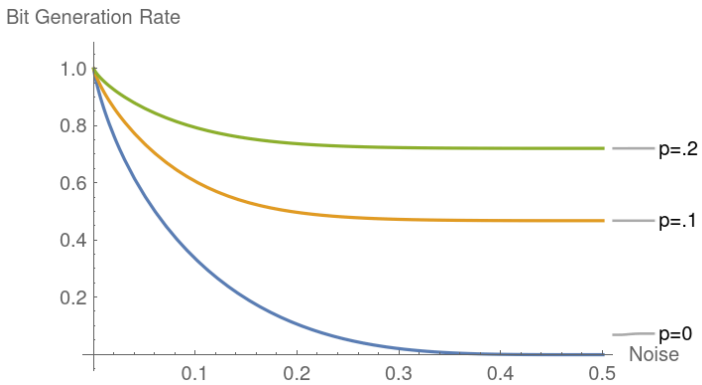

Figure 1. Showing the bit generation rate assuming natural noise is added at various levels of $p = 0$ (no natural noise added) to $p = .2$. x-axis indicates the observed adversarial noise before post-processing (i.e., before additional noise is added). We see here that natural noise can benefit the bit generation rates of source independent QRNG.

where $\langle e_0|f_0\rangle = 0$. From the above equation, it holds that $Re(\alpha) = 1 - 2Q_X$. Of course, $\beta = \sqrt{1-|\alpha|^2}$.

Now, consider a Distill round - Alice will measure in the Z basis causing the state to collapse to:

$$\sigma_{AE} = \frac{1}{2}|0\rangle\langle 0| \otimes |e_0\rangle\langle e_0| + \frac{1}{2}|1\rangle\langle 1| \otimes |e_1\rangle\langle e_1|. \tag{4}$$

Alice now performs the post processing using parameter p. This causes the final state to become:

$$\rho_{AE} = \frac{1}{2}|0\rangle\langle 0|_A \otimes ((1-p)|e_0\rangle\langle e_0| + p|e_1\rangle\langle e_1|) + |1\rangle\langle 1|_A \otimes ((1-p)|e_1\rangle\langle e_1| + p|e_0\rangle\langle e_0|). \tag{5}$$

At this point, we may compute $H(A|E)_\rho$. We may write ρ_{AE} in matrix form with respect to the basis $|0,e_0\rangle, |0,f_0\rangle, |1,e_0\rangle, |1,f_0\rangle$ and using Equation 3. This yields:

$$\begin{aligned}\rho_{AE} = &\frac{1}{2}\begin{pmatrix}1&0\\0&0\end{pmatrix}_A \otimes \left[(1-p)\begin{pmatrix}1&0\\0&0\end{pmatrix} + p\begin{pmatrix}|\alpha|^2 & \alpha^*\beta\\ \alpha\beta^* & |\beta|^2\end{pmatrix}\right] \\ &+ \frac{1}{2}\begin{pmatrix}0&0\\0&1\end{pmatrix}_A \otimes \left[p\begin{pmatrix}1&0\\0&0\end{pmatrix} + (1-p)\begin{pmatrix}|\alpha|^2 & \alpha^*\beta\\ \alpha\beta^* & |\beta|^2\end{pmatrix}\right]\end{aligned} \tag{6}$$

This decomposition allows us to easily compute the eigenvalues of ρ_{AE} and ρ_E, needed for $H(A|E)_\rho$ allowing us to compute the bit generation rate of the protocol in the asymptotic setting.

We must now, however, be careful of how the artificial noise is added. If the noise is *natural* - i.e., parameter p is dictated by some natural process, then the bit generation rate is exactly $\texttt{rate} = H(A|E)_\rho$. However, if the choice is artificial - namely, that Alice has to flip random coins herself to choose whether to keep or flip a bit - then this randomness must come from a pre-determined random string. This string may be refreshed, of course, using randomness generated after the protocol. However, the process of refreshing the random string must be taken into account. In this case, the rate becomes $\texttt{rate} = H(A|E)_\rho - h(p)$, as one needs, approximately $nh(p)$ bits of randomness in this case.

Figure 1 shows the bit generation rates for natural noise. We see that the higher the natural noise in the measurements, the more efficient the protocol becomes. This is different from the artificial noise case as shown in Figure 2 which clearly shows the more artificial noise added the lower the bit generation is. Even though Eve's uncertainty increases in the artificial noise case, the amount of extra seed randomness needed to choose to flip bits diminishes this advantage. Thus, while adding artificial noise clearly improves QKD,[14] we show here it does not help QRNG. Finally, a more direct comparison between natural and artificial noise is shown in Figure 3.

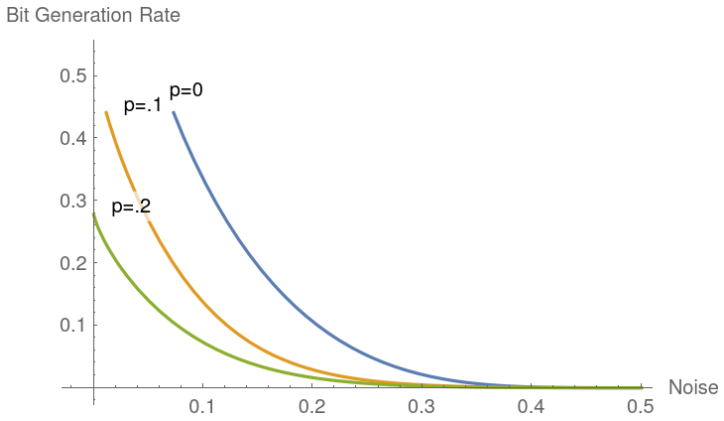

Figure 2. Showing the bit generation rate assuming artificial noise is added at various levels of $p = 0$ (no noise added) to $p = .2$. x-axis indicates the observed adversarial noise before post-processing (i.e., before additional noise is added). We see here that artificial noise does not benefit the bit generation rates of source independent QRNG. This is very unlike QKD where artificial noise does benefit.[14]

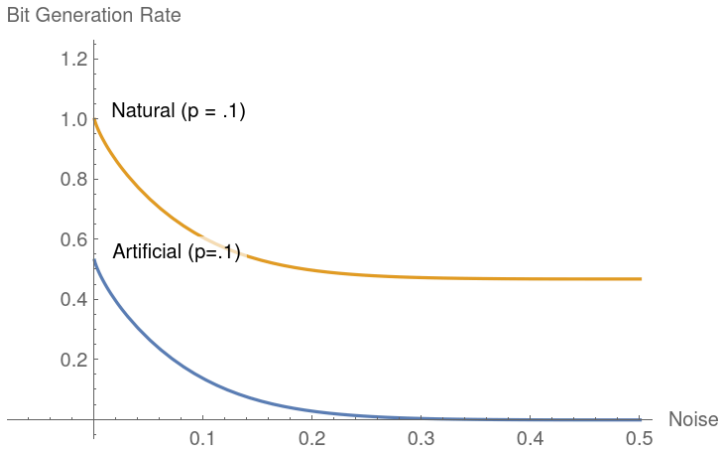

Figure 3. Comparing natural and artificial noise with $p = .1$.

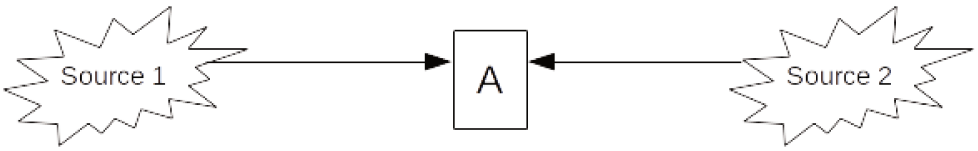

Figure 4. Diagram depicting the multi-source scenario for $\texttt{QRNG}_1$.

4.2 Multiple Sources

While the above strategy worked so long as the added noise was natural, if Alice was required to choose herself to add noise, the increased uncertainty Eve gained (which is good for Alice) did not compensate for the needed extra randomness that must be used and later refreshed. Thus, we next attempt to investigate whether an alternative source can be used to provide the extra randomness (see Figure 4). In particular, the signal from the first source is used to decide whether to flip the measurement result from the second source. In detail, given $r_1, r_2 \in \{0,1\}^n$, where r_1 is the Distilled string from the first source and r_2 from the second source, the post processing procedure operates as follows:

- For each $i = 1, \cdots, n$, if $r_1[i]$ (the i'th bit of r_1) is 0, then set $r'[i] = r_2[i]$; otherwise, set $r'[i] = 1 - r_2[i]$.

We assume each source is adversarial, but cannot collude at a quantum level (as in the multi-mediated security model introduced in[15] for QKD). Due to this, we can use our analysis in the previous section. Namely, the two sources prepare a state of the form:

$$|\psi_0\rangle = \frac{1}{2}(|0, e_0\rangle + |1, e_1\rangle) \otimes (|0, g_0\rangle + |1, g_1\rangle). \tag{7}$$

We may use the analysis in the previous section to discover:

$$Re\,\langle e_0|e_1\rangle = Re\,\langle g_0|g_1\rangle = 1 - 2Q_X. \tag{8}$$

Note that we are assuming the noise in both channels is the same - our analysis below can be followed and used assuming different channel noise levels, though we do not consider this case here. We may write the final density operator as:

$$\frac{1}{2}\,|0\rangle\,\langle 0|_A \otimes (\frac{1}{2}\,|e_0, e_0\rangle\,\langle e_0, e_0| + \frac{1}{2}\,|e_1, e_1\rangle\,\langle e_1, e_1|) + \frac{1}{2}\,|1\rangle\,\langle 1|_A \otimes (\frac{1}{2}\,|e_0, e_1\rangle\,\langle e_0, e_1| + \frac{1}{2}\,|e_1, e_0\rangle\,\langle e_1, e_0|) \tag{9}$$

Then, similar to the previous sub-section, we may write the density operator in matrix form easily using the following identities:

$$|e_0, e_0\rangle\,\langle e_0, e_0| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{10}$$

$$|e_0, e_1\rangle\,\langle e_0, e_1| = \begin{pmatrix} \alpha^2 & \alpha\beta & 0 & 0 \\ \alpha\beta & \beta^2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{11}$$

$$|e_1, e_0\rangle\,\langle e_1, e_0| = \begin{pmatrix} \alpha^2 & 0 & \alpha\beta & 0 \\ 0 & 0 & 0 & 0 \\ \alpha\beta & 0 & \beta^2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{12}$$

$$|e_1, e_1\rangle\,\langle e_1, e_1| = \begin{pmatrix} \alpha^4 & \alpha^3\beta & \alpha^3\beta & \alpha^2\beta^2 \\ \alpha^3\beta & \alpha^2\beta^2 & \alpha^2\beta^2 & \alpha\beta^3 \\ \alpha^3\beta & \alpha^2\beta^2 & \alpha^2\beta^2 & \alpha\beta^3 \\ \alpha^2\beta^2 & \alpha\beta^3 & \alpha\beta^3 & \beta^4 \end{pmatrix} \tag{13}$$

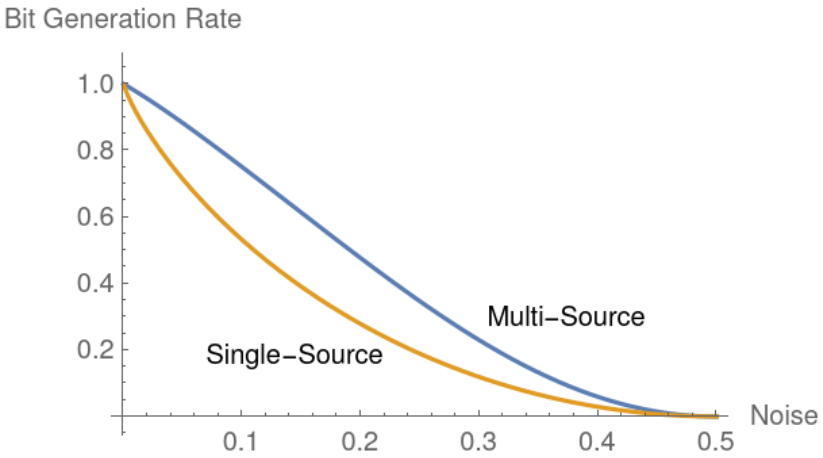

Figure 5. Comparing the bit generation rate of the multi-source protocol with the single-source version.

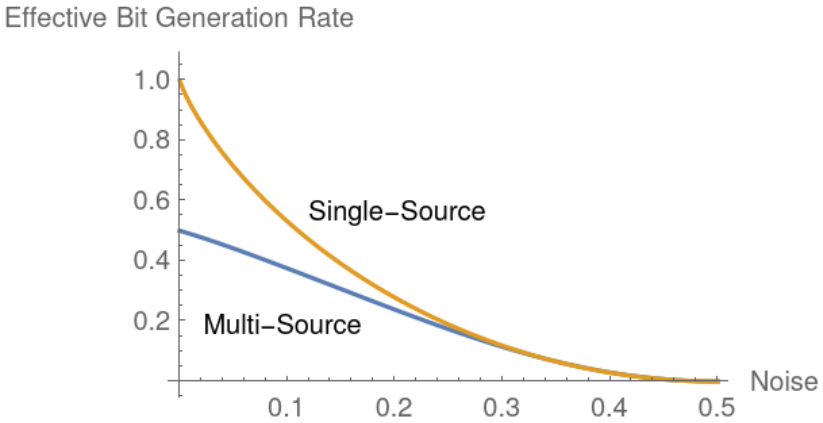

Figure 6. Comparing the *effective* bit generation rate of the multi-source protocol with the single-source version.

This lets us easily determine $H(A|E)_\rho$ by finding the eigenvalues of ρ_{AE} (we use Mathematica for this numerical computation). We note that, the bit generation rate for the multi-source scenario is higher than that of the single source as shown in Figure 5. However, the effective key-rate remains lower as shown in Figure 6. Thus, as with the previous post-processing method, while multi-sources help QKD, they do not always seem to benefit QRNG.

5. QUANTUM POST-PROCESSING

We now turn our attention to the second QRNG protocol which affords several interesting opportunities. While the above post processing methods may be applied to this protocol, we actually look into taking advantage of the Bell state and design novel *quantum* post processing methods. Let's first evaluate the bit generation rate of the protocol in the asymptotic setting. We consider the three basis variant (which gives statistics on the Z, X, and Y basis noise).

As before, we can consider collective attacks, using de Finetti style arguments to promote the security analysis to the general case. In this case, the source prepares multiple copies of the following state:

$$|\psi_0\rangle = \sum_{i=0}^{4} \sqrt{\lambda_i}\, |\phi_i\rangle \otimes |e_i\rangle\,. \tag{14}$$

Test rounds may be used to estimate Q_Z, Q_X, and Q_Y. Distillation rounds involve Alice measuring the first qubit in the Z basis and using the result as her raw random string (to be processed into a secret random string

through privacy amplification). We compute the density operator for such rounds to be:

$$\rho_{AE} = \frac{1}{2}|0\rangle\langle 0|_A \otimes \left[P\left(\sqrt{\lambda_0}|e_0\rangle + \sqrt{\lambda_1}|e_1\rangle\right) + P\left(\sqrt{\lambda_2}|e_2\rangle + \sqrt{\lambda_3}|e_3\rangle\right)\right] \tag{15}$$
$$+ \frac{1}{2}|1\rangle\langle 1|_A \otimes \left[P\left(\sqrt{\lambda_0}|e_0\rangle - \sqrt{\lambda_1}|e_1\rangle\right) + P\left(\sqrt{\lambda_2}|e_2\rangle - \sqrt{\lambda_3}|e_3\rangle\right)\right]$$

where $P(|z\rangle) = |z\rangle\langle z|$. We may assume the λ_i's are real and non-negative as any other phase may be absorbed into the $|e_i\rangle$ states. Furthermore, we may assume that the $|e_i\rangle$ states are orthonormal using methods in.[13] Given this state, let's consider the noise in the channel. It is clear the following identities hold:

$$Q_Z = \lambda_2 + \lambda_3$$
$$Q_X = \lambda_1 + \lambda_3$$
$$Q_Y = \lambda_1 + \lambda_2$$

From which we derive:

$$\lambda_1 = \frac{1}{2}(Q_X + Q_Y - Q_Z)$$
$$\lambda_2 = \frac{1}{2}(Q_Z + Q_Y - Q_X)$$
$$\lambda_3 = \frac{1}{2}(Q_Z + Q_X - Q_Y)$$
$$\lambda_0 = 1 - \lambda_1 - \lambda_2 - \lambda_3$$

Note that this forces $Q_Z \leq Q_X + Q_Y$, $Q_X \leq Q_Z + Q_Y$ and $Q_Y \leq Q_Z + Q_X$ (any other setting would represent a quantum state that could not be produced through the laws of quantum physics).

Given these identities, the value of $H(A|E)_\rho$ is easily computed from which the rate is also derived (namely, $\texttt{rate} = H(A|E)$). Note no pre-processing has been done yet. We observe something interesting, however, in that increasing the Z basis noise actually improves the overall performance! Note that increasing the X or Y basis noise actually hurts the performance of the system. Similar behavior was observed in[17] for QKD. See Figure 7. This opens up a new post-processing method: before measuring, Alice can perform an operation that increases Z basis noise without drastically increasing the X or Y basis noise. Namely, Alice can perform a quantum operation U before measuring her system which, ultimately, changes the λ values. Of course U must be unitary which restricts our options. We also note that the choice of U may depend on the observed noise in the Test rounds.

We have attempted to discover such post-processing strategies for cases when $Q_Z = Q_X = Q_Y$ however, were unable to do so (without requiring Alice to have quantum memory of her own). We are able to, however, find interesting strategies for cases when the noise is asymmetric. For example, assume $Q_Z = 0$ and $Q_X = Q_Y = Q$ for some non-zero Q. Note that this is a valid quantum channel as it obeys the constraints on the various noise levels discussed above. Let U be the following unitary map:

$$U|\phi_0\rangle = |\phi_0\rangle$$
$$U|\phi_1\rangle = \frac{1}{\sqrt{2}}|\phi_2\rangle + \frac{1}{\sqrt{2}}|\phi_3\rangle$$
$$U|\phi_2\rangle = |\phi_1\rangle$$
$$U|\phi_3\rangle = \frac{1}{\sqrt{2}}|\phi_2\rangle - \frac{1}{\sqrt{2}}|\phi_3\rangle$$

Applying this to Equation 14, yields:

$$|\psi_0\rangle = \sqrt{\lambda_0}|\phi_0, e_0\rangle + \sqrt{\lambda_1}(|\phi_2\rangle + |\phi_3\rangle)|e_1\rangle + \sqrt{\lambda_2}|\phi_1, e_2\rangle + \sqrt{\lambda_3}(|\phi_2\rangle - |\phi_3\rangle)|e_3\rangle = \sum_i \sqrt{\hat{\lambda}_i}|\phi_i, f_i\rangle,$$

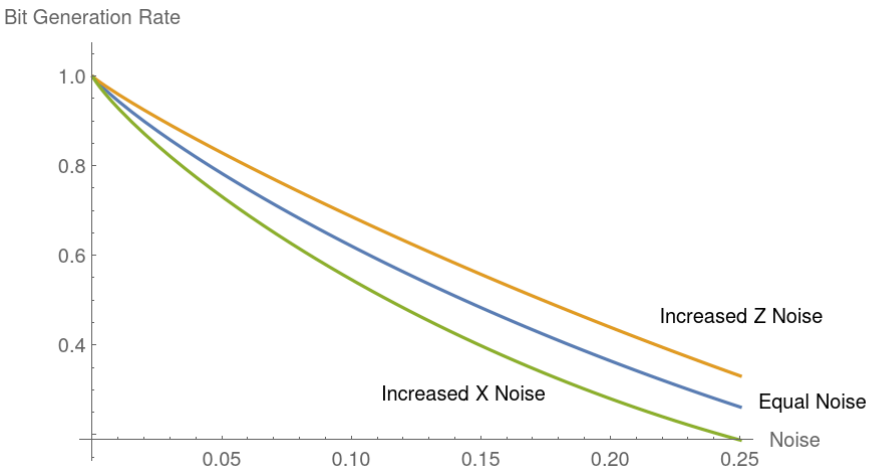

Figure 7. Showing how increasing the Z basis noise can actually improve performance of $\texttt{QRNG}_2$. Here, the x-axis is the overall noise parameter Q and we set $Q_Z = Q_X = Q_Y$ for the "Equal Noise" case; $Q_Z = 1.5Q$, $Q_X = Q_Y = Q$ for the "Increased Z noise" case; and $Q_X = 1.5Q$, $Q_Z = Q_Y = Q$ for the "Increased X noise" case.

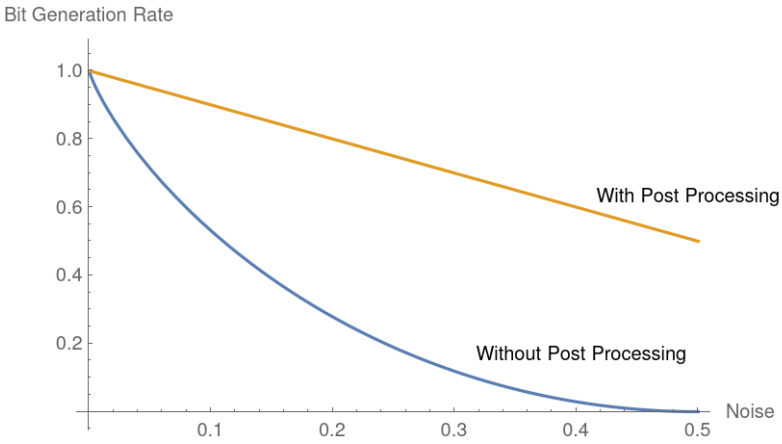

Figure 8. Showing how our quantum post processing strategy can benefit $\texttt{QRNG}_2$. Here, the x-axis is the adversarial noise parameter Q and we set $Q_Z = 0$ while $Q_X = Q_Y = Q$.

where:

$$\begin{aligned}
\hat{\lambda}_0 &= \lambda_0 \\
\hat{\lambda}_1 &= \lambda_2 \\
\hat{\lambda}_2 &= \frac{1}{2}(\lambda_1 + \lambda_3) \\
\hat{\lambda}_3 &= \frac{1}{2}(\lambda_1 + \lambda_3).
\end{aligned}$$

Now, given these new λ values, we have $\hat{Q}_Z = Q$, $\hat{Q}_X = Q/2 = \hat{Q}_Y$. (Note, these are the noise values of the state after post-processing whereas Q is the actual observed noise due to Eve.) We note that under these channel conditions the bit generation rate of the protocol is substantially improved with this post-processing method as shown in Figure 8. We also note that this method does not improve performance if the noise in the channel is identical in all basis. We leave it as an open question whether or not a suitable post-processing method, without requiring Alice to hold a quantum memory, can be found for symmetric noise channels.

6. CLOSING REMARKS

In this paper, we have analyzed two different source-independent QRNG protocols and shown how post-processing may be applied. Some post-processing strategies that work well in QKD scenarios do not always provide a benefit, and can actually hurt, QRNG as we show here. We also show how quantum post processing strategies can benefit in some instances. Many interesting open questions remain. Of particular interest would be to derive more quantum post processing strategies for other channel noise scenarios (we only considered one scenario here). Also performing these analyses in the finite-key setting is vitally important. We leave this as interesting future work.

Acknowledgments

The author would like to acknowledge support from NSF grant number 2143644.

REFERENCES

[1] Herrero-Collantes, M. and Garcia-Escartin, J. C., "Quantum random number generators," *Reviews of Modern Physics* **89**(1), 015004 (2017).

[2] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al., "Advances in quantum cryptography," *Advances in optics and photonics* **12**(4), 1012–1236 (2020).

[3] Amer, O., Garg, V., and Krawec, W. O., "An introduction to practical quantum key distribution," *IEEE Aerospace and Electronic Systems Magazine* **36**(3), 30–55 (2021).

[4] Colbeck, R. and Kent, A., "Private randomness expansion with untrusted devices," *Journal of Physics A: Mathematical and Theoretical* **44**(9), 095305 (2011).

[5] Pironio, S. and Massar, S., "Security of practical private randomness generation," *Physical Review A* **87**(1), 012336 (2013).

[6] Vallone, G., Marangon, D. G., Tomasin, M., and Villoresi, P., "Quantum randomness certified by the uncertainty principle," *Physical Review A* **90**(5), 052327 (2014).

[7] Xu, F., Shapiro, J. H., and Wong, F. N., "Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring," *Optica* **3**(11), 1266–1269 (2016).

[8] Haw, J.-Y., Assad, S., Lance, A., Ng, N., Sharma, V., Lam, P. K., and Symul, T., "Maximization of extractable randomness in a quantum random-number generator," *Physical Review Applied* **3**(5), 054004 (2015).

[9] Li, Y.-H., Han, X., Cao, Y., Yuan, X., Li, Z.-P., Guan, J.-Y., Yin, J., Zhang, Q., Ma, X., Peng, C.-Z., et al., "Quantum random number generation with uncharacterized laser and sunlight," *npj Quantum Information* **5**(1), 1–5 (2019).

[10] Xu, B., Chen, Z., Li, Z., Yang, J., Su, Q., Huang, W., Zhang, Y., and Guo, H., "High speed continuous variable source-independent quantum random number generation," *Quantum Science and Technology* **4**(2), 025013 (2019).

[11] Avesani, M., Marangon, D., Vallone, G., and Villoresi, P., "Secure heterodyne-based quantum random number generator at 17 gbps (2018)," *arXiv preprint arXiv:1801.04139* .

[12] Drahi, D., Walk, N., Hoban, M. J., Fedorov, A. K., Shakhovoy, R., Feimov, A., Kurochkin, Y., Kolthammer, W. S., Nunn, J., Barrett, J., et al., "Certified quantum random numbers from untrusted light," *Physical Review X* **10**(4), 041048 (2020).

[13] Renner, R., "Security of quantum key distribution," *International Journal of Quantum Information* **6**(01), 1–127 (2008).

[14] Renato, R., Gisin, N., and Kraus, B., "An information-theoretic security proof for qkd protocols," *Phys Rev A* **72**(1) (2005).

[15] Krawec, W. O., "Multi-mediated semi-quantum key distribution," in [*2019 IEEE Globecom Workshops (GC Wkshps)*], 1–6, IEEE (2019).

[16] Konig, R. and Renner, R., "A de finetti representation for finite symmetric quantum states," *Journal of Mathematical physics* **46**, 122108 (2005).

[17] Murta, G., Rozpedek, F., Ribeiro, J., Elkouss, D., and Wehner, S., "Key rates for quantum key distribution protocols with asymmetric noise," *Physical Review A* **101**(6), 062321 (2020).